ABSTRACT OF THE DISCLOSURE

A parallel block encryption method and modes (modes or operation) that provide both data confidentiality and integrity with a single cryptographic primitive and a single processing pass over the input plaintext string by using a non-cryptographic Manipulation Detection Code function for secure data communication over insecure channels and for secure data storage in insecure media. The block encryption method and modes of this invention allow, in yet a further aspect, parallel or pipelined operation of the block enciphering and deciphering functions in and architecture-independent manner. The present invention allows, in a further aspect, error recovery. In a yet further aspect, the present invention allows software and hardware implementations, and use in high-performance and low-power applications, and low-power, low-cost hardware devices. In a yet further aspect, the block encryption method and modes of this invention are suitable for real-time applications.